

National Provider Identifier (NPI)

The National Provider Identifier or NPI is a requirement of HIPAA, Administrative Simplification. The NPI is a single provider identifier that will replace the multiple provider identifiers currently used in healthcare transactions.

IMPORTANT NPI FACTS

- The NPI is a unique 10-digit number assigned for life to a healthcare provider or provider organization.
- Providers should **apply now** for an NPI. NPIs **must** be used in standard electronic healthcare transactions on and after **May 23, 2007**. Application can be made on paper or electronically. NPI information can be found at: <http://www.cms.hhs.gov/NationalProvIdentStand/>.
- CMS has issued an NPI transition plan, in effect from 1/3/2006 through 10/1/2006, when they will accept the NPI; the current Medicare number **must** also be present.
- Most commercial payers are still developing their NPI transition strategies. Watch for communications from them about NPI.

NPI ISSUES TO CONSIDER

Billing and Clinical Software Issues

- Verify that your software can handle the 10-digit NPI as well as your current ID wherever a provider identifier is required.
- Determine how your electronic claim is created -- by your billing system vendor or your clearinghouse. Talk to them about how the provider information is created.

Transition Issues

- Develop procedures concerning release of your NPI to other providers, as well as obtaining NPI from other providers.
- Protect your cash flow by staying informed of payer NPI transition timelines.

How does MHCC Promote EDI?

EDI Data Collection

COMAR 10.25.09 requires Maryland payers to submit healthcare transaction data to MHCC on an annual basis. MHCC analyzes and trends this data and publishes an annual EDI Progress Report. MHCC also provides consultative support to healthcare providers, payers and vendors.

Electronic Health Records

Electronic Health Records (EHRs) improve patient safety, quality of care, and administrative efficiencies using health information technology (HIT). Maryland has formed a 26-member task force to study the implementation of EHRs statewide.

Certification of Electronic Health Networks (EHNs)

EHNs (also known as claims clearinghouses) displaying this logo have been certified by MHCC and have demonstrated industry best practices in privacy, confidentiality, technical performance, business practices, and security.



Visit the MHCC website for more information about EDI
<http://mhcc.maryland.gov>

Maryland Health Care Commission
Stephen J. Salamon, Chairman
4160 Patterson Avenue, Baltimore, MD 21215
Tel: 410-764-3570, Fax: 410-358-1236



Electronic Data Interchange

Trends & Issues

Data Systems & Analysis
EDI Division

January 2006

What is EDI?

Electronic Data Interchange (EDI) is the computer application-to-application exchange of healthcare data in a standard format. Healthcare EDI includes the standard HIPAA transactions, such as claims, remittance, and eligibility, as well as the transmission of electronic prescriptions and clinical patient information. In 2004, almost 63% of Maryland private payer practitioner and hospital claims were sent electronically to payers.

Both federal and state government have implemented or are developing regulations and/or initiatives to standardize healthcare EDI and protect the privacy and security of healthcare information.

HIPAA Privacy Complaints

The federal Department of Health & Human Services, Office of Civil Rights (OCR), is responsible for HIPAA Privacy Rule enforcement and the protection of patient protected health information or PHI. As of November 30, 2005 they report:

-  16,625 privacy complaints filed since the April 2003 privacy effective date.
-  69% of complaints were resolved by the covered entity correcting the problem or because the complaint was not a privacy rule violation.
-  OCR referred more than 263 privacy violations to the Department of Justice for potential prosecution; one case has been successfully prosecuted.
-  The top five complaints against providers include violations of use or disclosure of PHI, lack of adequate PHI safeguards, refusal or failure to provide a patient access to records, disclosure of more information than necessary, and failure to obtain authorizations to disclose PHI.

HIPAA Compliance Tips

Protect Patient Email

If you use email to communicate with your patients, consider the following steps to safeguard patient PHI:

Educate Employees

Provide training to insure employees can identify PHI and it's proper release, disclosing only the minimum necessary information. Refrain from sending sensitive information relating to mental illness, substance abuse, or HIV tests. Maintain copies of patient emails in patient's medical record.

Safeguard your Emails

Protect the security of emails you send by obtaining email encryption software that securely encodes your emails and protects the information. Include a confidentiality disclaimer with all emails sent from your office.

Educate Patients

Obtain patient consent before sending emails to them. Educate your patients about emails and how you protect their information.

Protect Portable Devices

Portable devices, such as laptops, PDAs, or internet-enabled phones that you or your staff use may contain PHI and must be secured. Some suggestions include:

Identify Portable Devices

Meet with all staff members and catalog what devices are used, by whom, and how they are used both inside and outside the office.

Understand User Features

Understand the user features of portable devices and deactivate those features that may compromise patient PHI. Implement robust password protections and shorten the period of time that a device will lock when inactive.

Protect Computers

Strong user ID and password protection will limit what information is available to individual employees and prevent unauthorized access to patient information. Steps to secure these devices include:

Protect Passwords

Eliminate default passwords and implement a password expiration period of 90-120 days.

Issue Unique User IDs


Each staff member should have their own, unique user ID which limits the type of patient information they can access.

Define Password Formats

Enforce specific password formats. A length of eight or more digits with a combination of alpha, numeric and special characters is recommended.

Electronic Health Records

The use of health information technology (HIT) and electronic health records (EHR) is gaining momentum. The federal government and the private sector are actively pursuing initiatives to define, develop, and implement an interoperable HIT infrastructure that will improve the quality and efficiency of health care. Interoperability refers to the ability of two or more systems or components to exchange and use information. HIT initiatives include:

-  **Appointment** of Dr. David Brailer as head of the Office of the National Health Information Technology Coordinator to develop a national HIT infrastructure.
-  **Grants** to healthcare providers by the Agency for Healthcare Research and Quality (AHRQ) to implement HIT in medical offices.
-  **Development** of an EHR product certification program by the Certification Commission for Healthcare Information Technology (CCHIT). It will establish uniform vendor standards to help minimize provider risk when purchasing HIT applications.